

UNITED STATES PATENT APPLICATION

OF

Vsevolod M. Kuzmich and Igor O. Ivanov

For

**PROPRIETARY WATERMARK SYSTEM FOR
FOR SECURE DIGITAL MEDIA AND CONTENT DISTRIBUTION**

20020703 10:00:00

CROSS-REFERENCING TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 60/269,863, filed on February 21, 2001, in the name of inventors Vsevolod M. Kuzmich and Igor O. Ivanov, titled "Proprietary Watermark System for Secure Digital Media and Content Distribution", which is hereby incorporated by reference as if fully set forth herein.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention relates to media protection systems, and more particularly, to a digital media/content protection system that provides the protection of the media owner's copyright during a media/content distribution process using cryptographic and watermarking techniques.

Discussion of the Related Art

[0003] In today's digital world, there is a great wealth of information that can be accessed in various forms: text, image, audio, and video. The relationships within the digital content triangle, "Owner, Distributor, and Customer" have become more and more complicated. The electronic representation and transfer of the digital media and content have increased the potential for any misuse and theft of such information and have significantly increased the problems associated with the enforcement of the copyright protection of such information.

[0004] These problems are rooted from the intrinsic features of the digital information: making copies of the information is easy and inexpensive, each copy is identical to the original (no quality loss), and the distribution of the copies is easy and fast. For these reasons, the authors and publishers of multimedia materials fear providing their works in the multimedia services and are seeking the solutions that can eliminate the problems associated with the copyright protection of the multimedia data. Thus, to preserve the digital media originality and to provide the security and copyright of the media, their distribution became a very important issue. There are two major techniques that are involved when providing a protection of the digital media: cryptography and digital watermarking.

[0005] Cryptography is a technology that is widely used for providing the data security. Relating to digital media, cryptography is used to provide the security of the access to copyright information access among the media managers in the Owner-Distributor-Consumer triangle. There are two main classes of cryptographic systems: symmetric key and public key (asymmetric

key) encryption systems. A hybrid cryptographic system is a system in which both classes of systems are combined.

[0006] In a symmetric key encryption system, a single key can be used both to encrypt and decrypt. There are several efficient implementations of the symmetric key systems, but their key management is often troublesome.

[0007] In a public key encryption system, the processes of the data encryption and decryption are independent from each other. The data encryption process employs a public key, while the data decryption process requires a different (but mathematically related) private key. Knowing of the public key allows the encryption of a plaintext but does not allow the decryption of a ciphertext: the private key is necessary for the ciphertext decryption. A key owner keeps his private key secret so that he is the only person who can decrypt an encrypted ciphertext and sign the digital data using his private key. If the key owner publishes his public key, then anyone can use that key to encrypt messages for the key owner and to verify the owner signature.

[0008] In a hybrid cryptographic system, a plaintext is encrypted with a symmetric algorithm having a symmetric key. The symmetric key itself is encrypted with a public-key algorithm having a public key. The encrypted symmetric key and data are then delivered to a recipient, who uses his private key to decrypt the symmetric key and uses the decrypted key to decrypt the data. This process is considerably faster than a public key encryption system, and it allows using a different symmetric key each time, considerably enhancing the security of the symmetric algorithm. Thus, the hybrid cryptographic system is ideal for transferring the protected media to a user.

[0009] Digital watermarking is a technology that is used for embedding copyright information data into various forms of media such as image, audio, and video with a minimum amount of perceivable degradation of the "host" signal. The embedded data should be invisible and inaudible to a human observer. The digital watermarking technology is often used to modify the played and recorded media signals and to keep track of a list of the involved playing or recording devices in order to detect any illegal copy maker. Using the technology, one can distinguish legal media from the illegal media copies. The purpose of embedding the copyright information into the digital media is to provide a proof of the copyright and assurance of the content integrity. Therefore, the embedded data should stay stable in a host signal even if the host signal is processed. Such a hidden and stable data, securely placed into a "host" signal to store the essential supplementary information, is called a watermark.

[0010] A watermarking process includes three basic stages: generating a watermark, embedding the watermark, and detecting the watermark. A watermark belongs to one owner who is the only person who can proceed to prove the ownership of the host signal.

SUMMARY OF THE INVENTION

[0011] Accordingly, the present invention is directed to a copyright protection method for digital media in a media distribution process.

[0012] An object of the present invention is to provide a copyright protection method for digital media/content that (1) properly protects the copyrights of the media content owner, (2) reliably preserves and proves the originality of the digital media, and (3) provides the security of the media/content distribution process.

[0013] Additional advantages, objects, and features of the invention will be set forth in part in the description which follows and in part will become apparent to those having ordinary skill in the art upon examination of the following or may be learned from practice of the invention. The objectives and other advantages of the invention may be realized and attained by the structure particularly pointed out in the written description and claims hereof as well as the appended drawings.

[0014] To achieve these objects and other advantages and in accordance with the purpose of the invention, as embodied and broadly described herein, a first copyright protection method for digital media includes embedding a secrete watermark into an original media content, the secrete watermark being generated with a secrete key of a content owner and representing an authorization signature of the owner; embedding a first public watermark into the secrete watermark-embedded media content, the first public watermark being generated with a first private key of the owner and certifying a first copyright of the owner; and embedding a second public watermark into the first public watermark-embedded media content, the second public watermark being generated with a second private key of a content distributor and certifying a second copyright of the distributor.

[0015] In another aspect of the present invention, a second copyright method for digital media includes embedding a secrete watermark into an original media content, the secrete watermark being generated with a secrete key of a content owner and representing an authorization signature of the owner; embedding a first public watermark into the secrete watermark-embedded media content, the first public watermark being generated with a first private key of the owner and certifying a first copyright of the owner; embedding an informational watermark into the first public watermark-embedded media content, the informational watermark including additional information related to the original content; and embedding a second public watermark into the informational watermark-embedded media content, the second public watermark being generated with a second private key of a content distributor and certifying a second copyright of the distributor.

[0001] It is to be understood that both the foregoing general description and the following detailed description of the present invention are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this application, illustrate embodiment(s) of the invention and together with the description serve to explain the principle of the invention. In the drawings;

[0017] FIG. 1 is a flow chart illustrating the copyright protection method according to the present invention;

[0018] FIG. 2 is a flow chart illustrating a method of verifying the validity of a media content by using a secret proprietary watermarking technique according to the present invention; and

[0019] FIG. 3 is a flow chart illustrating a method of verifying the validity of a media content by using a public proprietary watermarking technique according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0020] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

[0021] The present invention relates to a copyright protection method of the digital media and the digital content distribution. It is applicable to all types of media, and the principles of the present invention may be extended by one having ordinary skill in the art to any new types. The present invention offers a high-level protection to multimedia right owners. It further offers a use of three subjects of digital media distribution process: a content owner, a content distributor, and a content consumer.

[0022] First of all, the content owner is a subject who produces and owns an original media copy (original content). The content owner can distribute the copies of the original content and certify his copyright by digitally signing the copies. Second, the content distributor is a subject who receives the copies of the original content from the content owner and has a right to redistribute the copies to one or more consumers or to other distributors. The content distributor can also certify his copyright by digitally signing the distributed content. Lastly, the content consumer is a subject who receives the copies of the original content from the content owner or content distributor for his or her personal use.

[0023] When a copyright owner signs the digital media materials produced, it is essential to choose a proper technique for digital content signing. One of the ways of signing a digital content is digital watermarking. Digital watermarking allows keeping the indelible marks within the media data, and these marks could be used to indicate the owner's copyright. The copyright must be distributed with the media content to indicate the content owner's right. The present invention offers to store the copyright data in the form of a digital watermark into the content. Each owner of the copy of the content can add his or her own watermark as an owner data indicating his or her copyright corresponding to the content.

[0024] The present invention offers three ways to protect the copyright of digital media during the digital media distribution in accordance with a secrecy level: secrete, public, and informational proprietary copyright protection schemes. A copyright protection method of the present invention is illustrated in FIG. 1. The system shown in FIG. 1 employs a combination of all of three schemes and can be used for the security level assignment among the content distribution participants. As mentioned above, the main parts of the content distribution participants are a content owner, a content distributor, and a content consumer.

[0025] The content owner adds a secrete watermark (owner secrete watermark) into an original media content using his own secrete key. The secrete watermark represents an owner authorization signature for the media content. This watermark can be distinguished only by the secrete key owner. Then, the content owner adds a public watermark (owner public watermark) that allows to certify the owner's right and to check it by any third party, who has an owner public key (public key 1). Additionally, the content owner adds an informational watermark that allows to store additional content information (content properties) within the media content. Anyone can read this information without any access key by using a special software tool.

[0026] After the content preparation processes described above are performed, the content owner hands the owner-watermarked content over to the content distributor. Then the content distributor adds his own public watermark (distributor public watermark) into the owner-watermarked content that allows to certify his copyright and to check it by any third party, who has a distributor public key (public key 2). The consumer can get an informational watermark without any key and any public watermark by using a corresponding public key.

[0027] FIG. 2 is a flow chart illustrating a method of verifying the validity of a media content by using the secrete proprietary watermarking technique according to the present invention. The secrete proprietary copyright protection scheme is based on the symmetric cryptography (using a secrete key) and digital watermarking principles. Secrete proprietary watermarks can be used as the authentication and content integrity mechanisms in a variety of ways. This implies that the watermark is a secured link and readable only by the authorized persons having the secrete key, which was used to generate the watermark. Removing this type

of watermark should be possible with a heavy degradation of the carrier signal. In order to detect this type of watermark, a secrete key and an owner identification (ID) must be known. Thus, only a content owner who knows the secrete key and owner ID is able to operate with a secrete proprietary watermark. The main goals of the method shown in FIG. 1 are as follows:

- Distinguish the presence of the watermark within the content and illicit copying disclosure
- Conserve ancillary owner information within watermarked content
- Protect owner information embedded into the content from unauthorized access and modifications

[0028] The requirements of the secrete proprietary copyright protection security are as follows:

- An appropriate symmetric key cryptography algorithm must be used.
- A digital watermarking technique that provides robust watermark embedding and detection must be used.
- It must be possible to authenticate a watermark message with only the watermarked content, the secrete watermarking key, and the owner ID.
- Authentication or the failure to authentication of the watermark message must survive the subsequent encoding with the same or other watermarking process.
- A digital watermarking system should be implementable by an individual content creator, where authentication of the watermarked content is possible by any third party.
- In a digitized form, the content should only be distributed with watermarks if the watermarks are expected to provide authentication.

[0029] This scheme assumes that the owner of the content has to specify some information for the watermarking process. The first part of the data is Delimiter generated on the basis of the owner ID. It allows to divide the different content owners' or redistributors' watermarks from each other. The second part of the data is owner data that the owner wants to associate with the current copy of the content. This is an information part of the watermark. The third part of the data is an owner secrete key (S_o) that is used as a basis of the symmetric cryptographic scheme protecting the watermark data itself from the illegal use.

[0030] A copyright protection apparatus compounds the watermark from the mentioned parts of the data in a manner that different content owners or redistributors have the different watermarks. The next step is to code each informational bit of the watermark according to the selected watermarking technique and embedding the obtained signal into the content. The owner ID is used to detect the watermark within the watermarked content. In a case of successful detection, the owner secrete key (S_o) must be produced to encode the watermark and obtain the plain owner data.

[0031] FIG. 3 is a flow chart illustrating a method of verifying the validity of a media content by using a public proprietary watermarking technique according to the present invention. The public proprietary copyright protection method is based on the public key cryptographic principles. By the definition, the public copyright protection embeds a traditional copyright notice into a signal with an owner private key. It is expected that the owner officially publishes the corresponding public key so that anyone can read it and check the watermark. Although the public copyright protection is bit less secure than a secret one, it is much more difficult to remove a visible/audible label. Moreover, the failure of the public watermark detection indicates that the signal has been significantly tampered, and the user can be informed of the alteration.

[0032] The main goals of the method shown in FIG. 2 are as follows:

- Distinguish the presence of the watermark within the content
- Conserve ancillary owner information (possibly including content properties) within the watermarked content
- Protect the owner information embedded into the content from any unauthorized access and modifications
- Provide any third party (having the public key) with an opportunity to get the content properties.

[0033] The requirements of the public copyright protection security are as follows:

- An appropriate symmetric-key cryptographic algorithm must be selected.
- A digital watermarking technique that provides the robust watermark embedding and detection must be selected.
- It must be possible to authenticate a watermark message with only the watermarked content, the public key and the owner ID.
- Authentication or a failure to authenticate of the watermark message must survive the subsequent encoding with the same or other watermarking processes.
- A digital watermarking system should be implemented by an individual content creator, where the authentication of the watermarked content can be done by any third party
- In a digitized form, the content should only be distributed with watermarks if the watermarks are expected to provide the authentication.

[0034] The public proprietary copyright protection shown in FIG. 3 assumes that the owner of the content has to specify some information for watermarking forming. The first part of the data is a delimiter generated on the basis of the owner identification (ID). It allows to divide the different content owners' or distributors' watermarks from each other. The second part is owner data that the owner wants to associate with the current copy of the content. This is an informational part of the watermark. The third part of the data is an owner public key (P_o) that

is used as a basis of an asymmetric cryptography scheme protecting the plain owner data itself from the illegal use.

[0035] The copyright protection system compounds the watermark from the mentioned parts of data in a manner that different content owners or redistributors have the different watermarks. The next steps are to code each informational bit of the watermark according to a selected watermarking technique and to embed the obtained signal into the content.

[0036] The owner ID and owner public key (P_o) are used to detect the watermark within the watermarked content, and in a case of successful detection, the owner public key (P_o) is used to encode the watermark and to obtain the plain owner data. The owner public key (P_o) and owner ID have to be passed to the content distributor or another content owner, and anyone who received the key can select and view the data that are concerned to the corresponding content owner or distributor.

[0037] The informational copyright protection scheme according to the present invention acts as an information carrier with the watermark readable to anyone. These watermarks are detectable by a third party using a special embedded tool of a media player (e.g., a Properties button). The informational watermarks mainly act as information links. Therefore, these links do not need to fulfill the same security constraints as the watermarks formed in the secrete copyright protection schemes. The information copyright protection scheme allows free validity detection: it does not need an original media data and any secrete key to determine the presence of a watermark.

[0038] The main goals of the scheme are to distinguish the presence of the watermark within the content and to inform a customer about the content owner and content properties (e.g., title, artist, date, version, media parameters such as bit-rate, and etc.).

[0039] Some of the requirements of the informational copyright protection security are as follows:

- An appropriate symmetric key cryptographic algorithm must be selected.
- A digital watermarking technique that provides the robust watermark embedding and detection must be selected.
- It must be possible to authenticate a watermark message with the watermarked content by using a special software module.
- A digital watermarking system should be implementable by an individual content creator, where the authentication of the watermarked content can be done by any third party.
- In a digitized form, the content should be distributed only with the watermarks if the watermarks are expected to provide authentication.

[0040] This scheme assumes that the content owner needs to specify some information for a public use. So, it is possible to associate the information with the content using a

watermarking technique without any cryptographic features. This information is related rather to the content itself than the content owner. No key is necessary to find and read the information.

[0041] If a content owner wants to redistribute the original content to a content distributor or another content owner with all the copyrights related to the content, it is possible to set Trusted Relationships between two parties. It means that the content owner has to pass his secrete key and owner ID to another party, e.g., by using a hybrid cryptographic scheme.

[0042] For confidentiality purposes, the message is (symmetrically) encrypted with a randomly generated session key, and this session key is encrypted with the public key of a receiver. This public-key-encrypted session key is sent along with the encrypted (symmetrical) message to the receiver. Then the receiver uses his private key to find the session key and decrypts the message using the found session key. By signing a short digest (hash) instead of the whole message, the integrity can be efficiently realized by a hybrid system.

[0043] It will be apparent to those skilled in the art that various modifications and variations can be made in the present invention without departing from the spirit or scope of the inventions. Thus, it is intended that the present invention covers the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.